CLAIMS

What is claimed:

1. A method for operating a data processing machine, comprising:

a) applying by a processor an encoding process to private-state data, where the private-state data captures a state of the processor;

b) writing, to a location in storage, said encoded private-state data, the location being one that is accessible to software that may be written for the processor; and

c) recovering the private-state data from the storage according to a decoding process that can undo the encoding process.

2. The method of claim 1 wherein the encoding process is to discourage an attempt at recovering the private-state data from the storage by a process other than the decoding process.

3. The method of claim 1 wherein the encoding process is only strong enough to cause an author of the software to apply, in writing said software, a technique prescribed by a manufacturer of the processor for accessing the private-state data from storage rather than circumventing said technique.

4. The method of claim 3 wherein the private-state data refers to one of

a) the content of an internal register of the processor that is not explicitly identified in an instruction manual for the processor that is intended for use by software developers, and

b) the content of an internal register of the processor that is explicitly identified in an instruction manual for the processor that is intended for use by software developers but is stored in one of a format and a location that is not explicitly identified in an instruction manual for the processor that is intended for use by software developers.

5. The method of claim 1 wherein the private-state data is written to one of a) a publicly accessible location in a register file of the processor b) cache, and c)memory.

6. The method of claim 1 wherein the encoding process is one in which the location of the written contents of a given internal register of the processor changes arbitrarily at least once, while repeating a)-b).

7. The method of claim 1 wherein the encoding process is one in which a storage format of the written contents of a given internal register of the processor changes arbitrarily at least once between big-endian and little-endian, while repeating a)-b).

8. The method of claim 1 wherein the encoding process is one in which a cipher is applied to the contents of a given internal register to produce an encoded value which is then written to the location in storage.

9. The method of claim 1 further comprising storing the recovered state data in a private storage of the processor.

10. An article of manufacture comprising:

a data processing machine having a private internal state, the internal state to change as the machine executes instructions provided to it as part of a program, wherein the machine is to encode data about the internal state and write the encoded state data to a location in a storage unit, wherein the location is accessible by an instruction set architecture of the machine .

11. The article of manufacture of claim 10 wherein the data processing machine is a processor that has a special read micro-operation, to be used when the processor is to recover said state data from the storage unit.

12. The article of manufacture of claim 11 wherein the processor further includes an internal cache and is to also write the encoded state data to a public location in the cache.

13. The article of manufacture of claim 11 wherein the processor is to recover the state data and write the recovered state data to a private location in the data processing machine.

14. The article of manufacture of claim 11 wherein the processor is to recover the state data and configure itself with the recovered state data in preparation for resuming execution of a suspended task.

15. The article of manufacture of claim 11 wherein the processor is one for which there is a manufacturer-defined instruction that, when executed by the processor, recovers the state data from the storage unit.

16. The article of manufacture of claim 10 wherein the data processing machine is a processor for which a special micro-operation is defined for accessing the encoded state data from the storage unit,

and wherein the processor further comprises an address obfuscation unit to receive an address value associated with given state data of the processor, the address value having been derived from a dispatch of the special micro-operation, the obfuscation unit to provide an encoded, physical address value that points to the actual location in the storage unit where the given state data is stored.

17. The article of manufacture of claim 10 wherein the data processing machine is a processor for which a hardware control signal is defined for accessing the encoded data from the storage unit,

and wherein the processor further comprises an internal cache, a data conversion unit to receive a data value from the internal cache as a result of a cache hit derived from the hardware control signal, the conversion unit to decode the data value into actual state data of the processor.

18. A computer system comprising:

a processor; and

a main memory communicatively coupled to the processor and having a public region designated to store the processor's private-state data in encoded form.

19. The system of claim 18 wherein the processor encodes the private-state data prior to storing it to the public region.

20. The system of claim 18 wherein the processor decodes a value read from the public region prior to using it.

21. The system of claim 18 wherein the processor further includes an internal storage unit in which a public region is designated to store a copy of said private-state data in encoded form.

22. The system of claim 21 wherein the internal storage unit is one of a cache and a register file.

23. The system of claim 21 wherein a private region is designated in the internal storage unit to store said private-state data in unencoded form.

24. The system of claim 18 further comprising a system chipset communicatively coupling the processor to the main memory.

25. A method for operating a data processing machine, comprising:
encoding private state data about a state of the machine; and
writing, to a location in storage, the encoded private state data, the location being accessible to software that is running on the machine.

26. The method of claim 25, wherein the encoding comprises ciphering a value of the private data to yield said encoded private data.

27. The method of claim 25, wherein the private data about the state of the machine is one of a register value and a value from the storage.

28. The method of claim 25, wherein the encoding comprises address encoding to obfuscate an address value of the private data.

29. The method of claim 25 further comprising:
recovering the private data from the storage according to a decoding process.

30. The method of claim 29 wherein the recovering comprises:
reading a plurality of values from memory; and
combining the read plurality of values to form a single unencoded value of said private data.

31. The method of claim 29 wherein the recovering comprises:

reading a plurality values from one or more discontiguous locations of memory;

combining the read plurality values to form a single value; and

decoding the single value to form an unencoded value of said private data.

32. The method of claim 25, the private data refers to one of a) the content of an internal register of the machine that is not explicitly identified in an instruction manual for the machine that is intended for use by software developers, and b) the content of an internal register of the machine that is explicitly identified in an instruction manual for the machine that is intended for use by software developers but is stored in a format or location that is not explicitly identified in an instruction manual for the machine that is intended for use by software developers.

33. The method of claim 29 further comprising storing the recovered private data in a private storage of the machine.